BEST AVAILABLE COPY

Claims

1. A method for provision of access for a data requesting entity (IRE) to
    data related to a principal, comprising the following steps:
-5-   creating an access granting ticket comprising
                (a) an access specification specifying a permission for an
                    access to data related to the principal, said data being
                    available at a data providing entity (IPE1),
                (b) a principal identifier representing the principal towards the
10   data providing entity (IPE1),
        -       encrypting the access granting ticket with an encryption key of
                the data providing entity (IPE1),
        -       communicating to the data requesting entity (IRE) the
                encrypted access granting ticket accompanied by an identifier
15   of the data providing entity (IPE1),
        -       communicating from the data requesting entity (IRE) to the
                data providing entity (IPE1) a request comprising the encrypted
                access granting ticket,
        -       decrypting the encrypted access granting ticket with a
20   decryption key of the data providing entity (IPE1)
                corresponding to the encryption key,
        -       providing to the data requesting entity (IRE) access to data
                related to the principal identifier according to the access
                specification.
25

2. The method according to claim 1, wherein the encrypted access granting
    ticket comprises or is accompanied by verification information and
    access is provided based on an analysis of the verification information.

30 3. The method according to claim 1 or 2, wherein the request to the data
    providing entity (IPE1) comprises a specification for requested data

related to the principal and access is provided according to a matching of the access specification and the requested data.

4. The method according to any of the preceding claims, wherein the access-granting-ticket-is-created-based-on-a-data storage correlating-at-least two items of a group comprising the identifier of the data providing entity (IPE1), the data related to the principal available at the data providing entity (IPE1), the principal identifier, the encryption key, and the access specification.

5. The method according to any of the preceding claims, wherein an indication for the access specification is entered into a principal entity (UE) to create the access granting ticket.

6. The method according to any of the preceding claims, wherein the access granting ticket further comprises security information and access is provided based on an analysis of the security information.

7. The method according to any of the preceding claims, wherein the encrypted access granting ticket is accompanied by public information.

8. The method according to claim 7, wherein the request to the data providing entity (IPE1) is communicated based on an analysis of the public information.

9. The method according to claim 7 or 8, wherein the decryption is based on an analysis of the public information.

10. The method according to any of the preceding claims, wherein the data to which access is provided to is transferred to the data requesting entity (IRE).

11. The method according to any of the preceding claims, wherein at least one further encrypted access granting ticket for further data related to the principal available at at least one further data providing entity (IPE2) is created and communicated to the data requesting entity (IRE) for provision of access to the further principal related data available at the at least one further data providing entity (IPE2), the at least one further encrypted access granting ticket being accompanied by at least one further identifier of the at least one further data providing entity (IPE2).

12. A principal entity (UE) for provision of access for a data requesting entity (IRE) to data related to a principal, comprising a transmission unit for sending of messages and information and a processing unit for processing of messages and information, wherein the processing unit is adapted to create an access granting ticket comprising an access specification specifying a permission for an access to data related to the principal, said data being available at a data providing entity (IPE1), and a principal identifier representing the principal towards the data providing entity (IPE1), to encrypt the access granting ticket with an encryption key of the data providing entity (IPE1), and to obtain an identifier of the data providing entity (IPE1), and the transmission unit is adapted to send the encrypted access granting ticket accompanied by the identifier of the data providing entity (IPE1) to the data requesting entity (IRE).

13. The principal entity (UE) according to claim 12, wherein the processing unit is adapted to include verification information into the access granting ticket and/or to attach verification information to the encrypted access granting ticket and the transmission unit is adapted to send the encrypted access granting ticket accompanied by the attached verification information to the data requesting entity (IRE).

14. The principal entity (UE) according to claim 12 or 13, wherein the processing unit is adapted to access a data storage correlating at least two items of a group comprising of the identifier of the data providing entity (IPE1), the data related to the principal available at the data providing entity (IPE1), the principal identifier, the encryption key, and the access specification, and to create the access granting ticket based on the data storage.

15. The principal entity (UE) according to any of the claims 12 to 14, wherein the processing unit is adapted to create the access granting ticket based on an indication for the access specification entered into an input unit of the principal entity (UE).

16. The principal entity (UE) according to any of the claims 12 to 15, wherein the processing unit is adapted to include security information into the access granting ticket.

17. The principal entity (UE) according to any of the claims 12 to 16, wherein the processing unit is adapted to obtain public information and the transmission unit is adapted to send the encrypted access granting ticket accompanied by the public information to the data requesting entity (IRE).

18. The principal entity (UE) according to any of the claims 12 to 17, wherein the processing unit is adapted to create at least one further encrypted access granting ticket for further data related to the principal available at at least one further data providing entity (IPE2) and the transmission unit is adapted to send the further encrypted access granting ticket to the data requesting entity (IRE) accompanied by at least one further identifier of the at least one further data providing entity (IPE2) for provision of

access to the further principal related data accessible at the at least one further data providing entity (IPE2).

19. A data requesting entity (IRE) comprising a receiving unit for receiving messages and information, a transmission unit for sending of messages and information, and a processing unit for processing of messages and information, the receiving unit is adapted to receive a first encrypted access granting ticket for provision of access to first data related to a principal, said first data being available at a first data providing entity (IPE1), the first encrypted access granting ticket being accompanied by an identifier of the first data providing entity (IPE1) and to receive a further encrypted access granting ticket for provision of access to further data related to the principal, said further data being available at a further data providing entity (IPE2), the further encrypted access granting ticket being accompanied by a further identifier of the further data providing entity (IPE2), the processing unit is adapted to generate a first request comprising the first encrypted access granting ticket and a further request comprising the further encrypted access granting ticket and the transmission unit is adapted to send the first request to the first data providing entity (IPE1) and the further request to the further data providing entity (IPE2), and the receiving unit is adapted to receive a first indication for access provision to the first data from the first data providing entity (IPE1) and a further indication for access provision to the further data from the further data providing entity (IPE2).

20. The data requesting entity (IRE) according to claim 19, wherein at least one of the first encrypted access granting ticket and the further encrypted access granting ticket is accompanied by public information and the processing unit is adapted to analyze the public information before the generation of at least one of the first request and the further request.

21. The data requesting entity (IRE) according to claim 19 or 20, wherein the first indication comprises the first data related to the principal and the further indication comprises the further data related to the principal.

22. A data providing entity (IPE1) for provision of access to data related to a principal, the data providing entity (IPE1) comprising a receiving unit for receiving messages and information, a transmission unit for sending of messages and information, and a processing unit for processing of messages and information, wherein the receiving unit is adapted to receive a request from a data requesting entity (IRE), the request comprising an access granting ticket encrypted with an encryption key of the data providing entity (IPE1), the access granting ticket comprising an access specification specifying a permission for an access to data related to the principal, said data being available at the data providing entity (IPE1), and a principal identifier representing the principal towards the data providing entity (IPE1); the processing unit is adapted to decrypt the encrypted access granting ticket with a decryption key of the data providing entity (IPE1) corresponding to the encryption key and to provide to the data requesting entity (IRE) access to data related to the principal identifier according to the access specification.

23. The data providing entity (IPE1) according to claim 22, wherein the encrypted access granting ticket comprises or is accompanied by verification information and the processing unit is adapted to provide access based on an analysis of the verification information.

24. The data providing entity (IPE1) according to claim 22 or 23, wherein the request comprises a specification for requested data related to the principal and the processing unit is adapted to provide access according to a matching of the access specification and the requested data.

25. The data providing entity (IPE1) according to any of the claims 22 to 24, wherein the access granting ticket further comprises security information and the processing unit is adapted to provide access based on an analysis of the security information.

26. The data providing entity (IPE1) according to any of the claims 22 to 25, wherein the encrypted access granting ticket is accompanied by public information and the processing unit is adapted to initiate the decryption based on an analysis of the public information.

27. The data providing entity (IPE1) according to any of the claims 22 to 26, wherein the transmission unit is adapted to send the data, to which access is provided to, to the data requesting entity (IRE).

28. A computer program loadable into the processing unit of a principal entity, wherein the computer program comprises code adapted to create an access granting ticket comprising an access specification specifying a permission for an access to data related to the principal, said data being available at a data providing entity (IPE1), and a principal identifier representing a principal towards the data providing entity (IPE1), to encrypt the access granting ticket with an encryption key of the data providing entity (IPE1), to obtain an identifier of a data providing entity (IPE1), and to initiate a sending of the encrypted access granting ticket accompanied by the identifier of the data providing entity (IPE1) to the data requesting entity (IRE).

29. A computer program loadable into the processing unit of a data requesting entity (IRE), wherein the computer program comprises code adapted to process a first encrypted access granting ticket for provision of access to first data related to a principal, said first data being available at a first data providing entity (IPE1), the first encrypted access granting

ticket being accompanied by an identifier of the first data providing entity (IPE1) and to process a further encrypted access granting ticket for provision of access to further data related to the principal, said further data being available at a further data providing entity (IPE2), the further encrypted access granting ticket being accompanied by a further identifier of the further data providing entity (IPE2), to generate a first request comprising the first encrypted access granting ticket and a further request comprising the further encrypted access granting ticket and to initiate a sending of the first request to the first data providing entity (IPE1) and of the further request to the further data providing entity (IPE2), and to process a first indication for access provision to the first data from the first data providing entity (IPE1) and a further indication for access provision to the further data from the further data providing entity (IPE2).

30. A computer program loadable into the processing unit of a data providing entity (IPE1), wherein the computer program comprises code adapted to process a request from a data requesting entity (IRE), the request comprising an access granting ticket encrypted with an encryption key of the data providing entity (IPE1), the access granting ticket comprising an access specification specifying a permission for an access to data related to a principal, said data being available at the data providing entity (IPE1), and a principal identifier representing the principal towards the data providing entity (IPE1), to decrypt the encrypted access granting ticket with a decryption key of the data providing entity (IPE1) corresponding to the encryption key and to provide to the data requesting entity (IRE) access to data related to the principal identifier according to the access specification.

31. The computer program according to any of the claims 28 to 30, wherein the computer program comprises code adapted to perform any of the steps of a method according to any of the claims 1 to 11.